LA GUERRA INFORMÁTICA
PARTE 2

Claudio Lopez

La guerra informática parte 2: La Metamorfosis de la Guerra Informática, el conflicto “permanente”

Autor: Lic. Claudio López – UNDEF

Reseño del autor:

El Lic. Claudio Lopez, es Magister en Ciberdefensa por la Facultad de Ingeniería del Ejército y Magíster en Ingeniería del Software por el ITBA y la Universidad Politécnica de Madrid, además posee una especialización en Criptografía y Seguridad Informática. Cuenta con una extensa trayectoria profesional en la Armada Argentina donde se desempeñó como Jefe del Servicio de Informática de la Armada y en el Estado Mayor Conjunto donde ocupo cargos en la Direccion General de Comunicaciones e Informática (ex Jefatura VI) ,

En el ámbito académico, es Director académico y docente de los cursos de posgrado en Análisis de Sistemas Automatizados para la ejecución de operaciones militares y para la gestión de la Defensa, Producción y Logística en la Facultad de la Armada (UNDEF). Sus investigaciones actuales se centran en el uso de redes neuronales e Inteligencia Artificial como herramientas de asesoramiento en la ciberatribución y la defensa ante ciberataques. Es autor del libro "Inteligencia Artificial en la Ciberdefensa" y de numerosos artículos sobre sistemas autónomos y guerra informática.

Resumen

El documento analiza la evolución de la guerra informática desde 2007, año en que fue desarrollado y publicado por este mismo autor un artículo referido a la guerra informática. En ese entonces se veía al ciberespacio como un nuevo entorno de desarrollo de las operaciones militares

Esta perspectiva inicial destacaba el surgimiento de la ciberguerra como un subcampo de las operaciones de información, donde se distinguían claramente las acciones ofensivas de las defensivas, y se subrayaba la importancia de objetivos como el comando y control, las comunicaciones y los sistemas de inteligencia.

Con el paso del tiempo, el enfoque sobre el ciberconflicto ha evolucionado y se ha vuelto mucho más complejo y multidimensional. La tecnología y el uso masivo de

Internet han cambiado radicalmente la forma en que se libran estos conflictos, incorporando nuevas dimensiones como la manipulación de la información y la influencia sobre la opinión pública.

Por lo tanto, el presente articulo explica cómo la estrategia actual, basada en el compromiso persistente y la defensa avanzada, implica operar de forma continua en redes adversarias, fusionando inteligencia, defensa y campañas de influencia. Además, resalta la importancia de la cooperación internacional y la colaboración entre sectores para enfrentar amenazas globales en un entorno digital donde los límites entre paz y guerra son cada vez más difusos.

Por otro lado, en este escenario de conflicto permanente, la inteligencia artificial (IA) ha emergido como un elemento transformador en la guerra informática. Los algoritmos de IA permiten automatizar tanto la detección de amenazas como la respuesta ante ataques, lo que eleva la velocidad y la precisión de las operaciones cibernéticas. Además, las herramientas de aprendizaje automático facilitan el análisis masivo de datos, optimizando la identificación de patrones maliciosos y anticipando estrategias adversarias. La IA, por ende, no solo refuerza las capacidades defensivas, sino que también potencia las campañas de influencia y manipulación de información, convirtiéndose en un componente fundamental de la competencia digital entre actores estatales y privados.

Abstract

This document analyzes the evolution of cyberwarfare since 2007, the year in which this author developed and published an article on cyberwarfare. At that time, cyberspace was viewed as a new environment for military operations.

This initial perspective highlighted the emergence of cyberwarfare as a subfield of information operations, clearly distinguishing between offensive and defensive actions and emphasizing the importance of objectives such as command and control, communications, and intelligence systems.

Over time, the approach to cyberconflict has evolved and become much more complex and multidimensional. Technology and the widespread use of the Internet have radically changed the way these conflicts are waged, incorporating new dimensions such as information manipulation and influencing public opinion.

Therefore, this article explains how the current strategy, based on persistent engagement and advanced defense, involves continuously operating in adversarial networks, merging intelligence, defense, and influence campaigns. Furthermore, it highlights the importance of international cooperation and cross-sector collaboration

to confront global threats in a digital environment where the lines between peace and war are increasingly blurred.

Furthermore, in this scenario of permanent conflict, artificial intelligence (AI) has emerged as a transformative element in cyberwarfare. AI algorithms make it possible to automate both threat detection and attack response, increasing the speed and precision of cyber operations. Furthermore, machine learning tools facilitate massive data analysis, optimizing the identification of malicious patterns and anticipating adversarial strategies. AI, therefore, not only strengthens defensive capabilities but also empowers influence campaigns and information manipulation, becoming a fundamental component of digital competition between state and private actors.

Introducción

El artículo de 2007 "La Guerra Informática", publicado en el Boletín del Centro Naval Nº 817 Pág. 219 de ese mismo año, cuyo autor es el que suscribe, ofrece una visión general de lo que entonces era un ámbito emergente del conflicto. Se categorizaba las “operaciones informáticas” en ofensivas y defensivas, siendo las ofensivas aquellas vinculadas a la propagación de virus, la manipulación de datos y la guerra psicológica a través de internet, a la vez que se definía a las operaciones defensivas como la protección de redes y sistemas.[1]

Sin embargo, el panorama de la ciberguerra ha evolucionado drásticamente desde entonces. Un análisis contemporáneo requiere un cambio de enfoque desde los conceptos fundamentales, hacia la naturaleza compleja, multidimensional y generalizada del ciberconflicto moderno.

La evolución tecnológica y el aumento exponencial del uso de Internet han redefinido por completo la manera en que se libran los conflictos en el ciberespacio. Hoy, la guerra informática no solo abarca operaciones ofensivas y defensivas, sino que también incluye la manipulación de la información y la influencia sobre la opinión pública, aspectos que han adquirido una importancia estratégica sin precedentes. Así, también la competencia entre estados y actores privados se ha intensificado, generando un entorno donde la innovación constante es clave para mantenerse a la vanguardia.

Por ejemplo, hoy un administrador de sistemas de una empresa ya no se enfrenta a un archivo malicioso estático, sino que puede ser objeto de un ataque orquestado por una Inteligencia Artificial generativa. En cuestión de segundos, una IA puede analizar el perfil psicológico de los empleados para lanzar una campaña de phishing hiperpersonalizada, mientras un malware evolutivo altera su propia firma digital en tiempo real para volverse invisible ante los antivirus convencionales. Al mismo tiempo, en las redes sociales de los ciudadanos, un deepfake de un líder

político, creado con una perfección inédita, comienza a viralizarse para erosionar la confianza pública y polarizar a la sociedad.

Para visualizar de manera clara este nuevo escenario con los conceptos fundamentales establecidos en 2007, la siguiente tabla detalla las diferencias clave entre la perspectiva inicial y la complejidad del escenario contemporáneo, donde la innovación constante es el único camino para mantener la iniciativa estratégica:

Tabla 1: Evolucion ciberconflicto

Característica	Visión 2007	Realidad 2025
Actor Principal	Hackers	APTs estatales y Cibermercenarios
Objetivo	Comando y Control	Infraestructura crítica y mente humana
Estrategia	Ofensiva/Defensiva discreta	Compromiso persistente (Defensa avanzada)
Herramienta	Virus y manipulación de datos	IA, Deepfakes y Malware evolutivo

Más allá de la ofensiva y la defensa: La era del compromiso persistente

Una perspectiva más actual, va más allá de la simple dicotomía entre ataque y defensa presentada en aquel artículo de 2007. El modelo estratégico actual, adoptado particularmente por las naciones líderes en capacidades cibernéticas, se basa en el compromiso persistente y la defensa avanzada. El General Nakasone argumenta en la publicación “Una Fuerza Cibernética para Operaciones Persistentes” (2019) que, para competir eficazmente, las fuerzas cibernéticas deben buscar continuamente la iniciativa táctica y estratégica, operando de manera global y continua contra los adversarios [2]. Esta doctrina postula que, para defender eficazmente sus redes, una nación debe operar continuamente dentro de las redes del adversario. Esto representa una evolución significativa sobre operaciones ofensivas y defensivas discretas

Este enfoque reconoce que el ámbito digital es un campo de batalla constante, sin una distinción clara entre tiempos de paz y tiempos de guerra. Las operaciones no se limitan a alterar o destruir datos, como se menciona en el texto de 2007, sino a recopilar inteligencia, posicionarse para futuros ataques y ejecutar campañas de influencia que no alcanzan el umbral del conflicto armado.

Este cambio implica que la defensa ya no se concibe como una barrera pasiva, sino como una actividad dinámica que requiere vigilancia constante, anticipación y respuesta proactiva. La estrategia de compromiso persistente

reconoce que las amenazas evolucionan a gran velocidad y que la detección temprana de intrusiones, junto con la capacidad de contrarrestar o incluso disuadir ataques dentro de las redes enemigas, es fundamental para la seguridad nacional. En consecuencia, las operaciones cibernéticas se desarrollan en un ciclo continuo de operación, donde la recopilación de inteligencia, la disrupción y el análisis forense son procesos simultáneos y entrelazados. Este punto introduce la necesidad de colaboración interinstitucional y alianzas internacionales, ya que la naturaleza global del ciberespacio hace que los ataques puedan provenir de cualquier lugar y afectar a múltiples sectores. Por ello, la cooperación y el intercambio de información entre gobiernos, empresas y organismos de seguridad se han convertido en pilares esenciales de la defensa cibernética moderna.

Jeff Kosseff, examina la estrategia de "defensa avanzada" desde la perspectiva del derecho internacional. Define el concepto como un conjunto de tres componentes: (1) posicionamiento para degradar operaciones adversarias, (2) advertencia para recopilar información, y (3) influencia para disuadir a los adversarios. [4]

Esta visión, desde el derecho internacional, subraya la importancia de equilibrar la protección con el respeto a normas globales, y pone en el centro el desafío de disuadir adversarios sin caer necesariamente en el enfrentamiento directo. En el contexto actual, donde las fronteras entre la guerra y la paz son cada vez más difusas, esta perspectiva invita a repensar la defensa como un ciclo continuo de inteligencia, prevención y persuasión.

Figura 1: Comando Conjunto de la CIberfensa

Los nuevos actores: De la habitación del hacker a las corporaciones del espionaje. El auge de los cibermercenarios

En el artículo de 2007 se identificaba como actores relevantes a los "hackers" motivados por intereses ideológicos o políticos, quienes simpatizaban con una causa específica. Un ejemplo de ello se observó durante la guerra serbobosnia, donde estos individuos empleaban ataques informáticos para apoyar a sus respectivos bandos, utilizando el ciberespacio como un recurso adicional en el conflicto.

Hoy en día, las principales amenazas son mucho más sofisticadas. Los principales actores son las “Amenazas Persistentes Avanzadas (APTs)” [3], que suelen ser grupos patrocinados por estados con importantes recursos, talento y objetivos estratégicos. Estos grupos, como APT28 (Rusia), el Grupo Lazarus (Corea del Norte) y varias APTs chinas, son responsables de importantes campañas de espionaje y sabotaje.

Además, el auge de los cibermercenarios o los grupos de Ransomware como Clop o Akira han comercializado la ciberguerra. Estos actores no estatales pueden ser contratados por naciones o corporaciones o actuar de forma independiente para paralizar infraestructuras críticas con fines lucrativos, difuminando la línea entre la actividad estatal y la delictiva.

Los mismos constituyen equipos de expertos, muchas veces organizados como empresas privadas que ofrecen sus servicios, ya sea para realizar ataques, desarrollar herramientas maliciosas o incluso brindar asesoría en ciberinteligencia. Estas entidades actúan ampliando el espectro de amenazas y dificultando la atribución de los ataques.

NSO Group, [5] empresa israelí fundada en 2010, desarrolla Pegasus, un software espía capaz de extraer datos personales de teléfonos inteligentes. NSO afirma que vende Pegasus solo a agencias gubernamentales para combatir el crimen y terrorismo. Sin embargo, investigaciones han revelado su uso para espiar a periodistas, abogados, disidentes y activistas, generando polémica internacional por violaciones a derechos humanos.

Black Cube , [6] otra agencia de inteligencia privada fundada en 2010 por ex agentes israelíes, con sedes en Tel Aviv, Londres y Madrid, se especializa en inteligencia para litigios, recopilando pruebas y rastreando activos, combinando agentes de campo e inteligencia cibernética. Ha estado envuelta en controversias por investigar a denunciantes de Harvey Weinstein y por operaciones de espionaje político.

En paralelo, ha surgido un mercado clandestino de exploits y datos robados, facilitando que incluso actores con recursos limitados puedan acceder a

capacidades avanzadas. La convergencia entre intereses estatales, económicos y delictivos ha generado un ecosistema donde la colaboración y el intercambio de técnicas es común, incrementando la complejidad de la defensa y la necesidad de estrategias flexibles y adaptativas.

Google Threat Analysis Group (TAG) en “Buying Spying: How the commercial surveillance industry works and what can be done about it ” (2024) ofrece una visión técnica y de mercado sobre los cibermercenarios. Explica cómo estas empresas desarrollan y venden herramientas de hackeo a operadores gubernamentales y no gubernamentales, y cómo sus acciones ponen en riesgo la seguridad de internet. El documento clasifica los tipos de actores y las cadenas de explotación que utilizan, basándose en la inteligencia de amenazas recopilada por Google.[8]

Esta diversificación de actores y tácticas ha obligado a los estados a desarrollar capacidades más sofisticadas de ciberinteligencia y respuesta. Los marcos legales internacionales se ven cada vez más desafiados para adaptarse a la velocidad y anonimato de estos ataques, mientras que la atribución precisa de los mismos se convierte en un reto técnico y diplomático considerable. Así, la disuasión y la resiliencia digital pasan a ser elementos prioritarios en la planificación de la seguridad nacional, promoviendo inversiones en infraestructura cibernética, formación de especialistas y cooperación global para hacer frente a amenazas multidimensionales.

Figura 2: Shalev Hulio CEO de NSO Group, Fuente: Clarin.com

El campo de batalla ampliado: Infraestructura crítica y guerra cognitiva

En el artículo de 2007 se identifica la infraestructura como un objetivo clave. Sin embargo, la realidad ha resultado más alarmante que el riesgo teórico de 2007. Eventos posteriores al artículo han demostrado las consecuencias tangibles y reales de los ciberataques a sistemas críticos:

Stuxnet (2010): Este sofisticado gusano, ampliamente atribuido a un esfuerzo conjunto entre Estados Unidos e Israel, dañó físicamente centrifugadoras nucleares iraníes mediante la manipulación de los sistemas de control industrial (ICS). Este evento histórico demostró que un arma digital podía causar efectos cinéticos.

The Shamoon-Attack I y II (2012) El 15 de agosto de 2012, Saudi Aramco tuvo que aislar su red informática tras un ataque con malware Disttrack, que afectó a 35.000 computadoras y puso en riesgo el suministro del 10% del petróleo mundial. El virus se propagó en la red y borró archivos antes de reescribir el Master Boot Record, dejando la empresa una semana sin servicios. Aunque EE. UU. señaló a Irán como responsable, no hay pruebas concluyentes; ambos países mantienen tensiones ideológicas y geopolíticas desde 1979.

Yellowstone 1 (2014): En 2014, hackers presuntamente iraníes atacaron el casino Las Vegas Sands Corp. en represalia por declaraciones polémicas de su CEO sobre Irán. El ataque, realizado mediante una "bomba de malware" que explotó las credenciales de un empleado, paralizó gran parte de los sistemas informáticos de la empresa en Las Vegas, afectando servidores, correos electrónicos, teléfonos y operaciones tecnológicas clave [10].

Ataques a la red eléctrica de Ucrania (2015, 2016): Hackers rusos respaldados por el Estado lograron desconectar partes de la red eléctrica de Ucrania, dejando a cientos de miles de personas sin electricidad en pleno invierno.

Ataque de ransomware al oleoducto Colonial (2021): El ataque de ransomware de un grupo criminal contra un importante operador de oleoductos de EE. UU. provocó escasez de combustible en la Costa Este, lo que demuestra la vulnerabilidad de la infraestructura privada a actores no estatales y el potencial de una disrupción social generalizada.

Más allá de la infraestructura física, la nueva frontera es la guerra cognitiva. Si bien el artículo original de 2007 aborda la guerra psicológica a través de internet, el enfoque moderno es más sistémico. Implica el uso de redes sociales, deepfakes y campañas coordinadas de desinformación para erosionar la confianza pública, polarizar las sociedades e influir en los procesos democráticos, convirtiendo el propio espacio informativo en un dominio disputado.

Según Irene Pujol (2024) la guerra cognitiva es un nuevo dominio de conflicto donde la mente humana es el campo de batalla. Sostiene que, en lugar de la fuerza física, se utilizan la psicología y la tecnología para manipular la percepción e influir en la toma de decisiones. Aprovecha los "atajos mentales" y sesgos cognitivos del cerebro para alcanzar objetivos estratégicos sin recurrir a la acción militar convencional, destacando la necesidad de entender y abordar las vulnerabilidades de nuestro sistema cognitivo.[9] El reconocimiento de estas vulnerabilidades es crucial en la era de la guerra cognitiva, ya que la defensa efectiva no solo requiere proteger sistemas tecnológicos, sino también fortalecer la capacidad de análisis crítico y resiliencia psicológica de la sociedad frente a intentos de manipulación masiva.

Así como los hackers tradicionales buscan errores de software para acceder a sistemas, quienes practican el “hacking humano” se enfocan en identificar y manipular esos "atajos mentales" y sesgos cognitivos que guían nuestras decisiones cotidianas. Estos sesgos, como la tendencia a confiar en la información repetida o a seguir la opinión mayoritaria, funcionan como verdaderas "puertas traseras" cognitivas que pueden ser explotadas para influir en el comportamiento, la percepción y la toma de decisiones de individuos o grupos.

La sofisticación de estas tácticas cognitivas se ha visto incrementada por la automatización y el uso de inteligencia artificial, permitiendo segmentar audiencias con precisión, adaptar mensajes en tiempo real y amplificar narrativas a gran escala. De este modo, los adversarios no solo buscan sabotear infraestructuras, sino manipular percepciones colectivas y provocar respuestas sociales predecibles, afectando la cohesión interna de los países objetivo. Así, la defensa ya no solo debe proteger sistemas físicos o digitales, sino también blindar el tejido social frente a ataques que explotan la psicología y la información, consolidando la guerra cognitiva como un eje central en la competencia entre estados y actores no estatales.

IA y automatización: el futuro del ciberconflicto

La naturaleza de la ciberguerra está siendo transformada por la inteligencia artificial (IA). Tanto atacantes como defensores están aprovechando estas tecnologías para automatizar y acelerar sus operaciones.

La IA se puede usar para crear malware altamente adaptable que cambia su código para evadir la detección, realizar reconocimientos automatizados de redes objetivo y ejecutar ataques también automatizados que identifican y explotan vulnerabilidades en tiempo real.

Por otro lado, la IA permite detectar patrones anómalos en grandes volúmenes de tráfico, anticipar movimientos maliciosos y responder a incidentes con mayor rapidez y precisión.

El despliegue de sistemas inteligentes en ambos frentes está redefiniendo el ritmo y la escala del ciberconflicto, haciendo que las amenazas evolucionen constantemente y obligando a las organizaciones a invertir en tecnologías de vanguardia y actualización continua de sus capacidades. En este escenario, la automatización y el aprendizaje automático se posicionan como herramientas indispensables tanto para la protección de infraestructuras críticas como para la gestión eficaz de la guerra cognitiva y la defensa nacional.

Conclusiones

El análisis presentado a lo largo de este artículo evidencia que la evolución del ciberconflicto ha dejado de ser un fenómeno marginal o estrictamente técnico para convertirse en un eje central de las relaciones internacionales contemporáneas. Los ejemplos históricos, desde Stuxnet, pasando por los ataques a la red eléctrica de Ucrania, hasta el ransomware que afectó al oleoducto Colonial, demuestran que tanto actores estatales como no estatales cuentan hoy con la capacidad de provocar daños físicos, disrupciones económicas y crisis sociales a través del ciberespacio. Estos incidentes no solo revelan la vulnerabilidad de infraestructuras críticas, sino que subrayan la creciente sofisticación y creatividad de los adversarios, quienes aprovechan la interconectividad global para ejecutar operaciones con consecuencias concretas y, muchas veces, impredecibles.

Sin embargo, el artículo trasciende el análisis de la infraestructura física y se adentra en la que probablemente sea la nueva frontera de la guerra: el dominio cognitivo. La guerra cognitiva, impulsada por la masificación de las redes sociales, la aparición de deepfakes y el desarrollo de campañas de desinformación, representa una amenaza que no se dirige únicamente a sistemas técnicos, sino directamente al núcleo de la cohesión social y la confianza pública. En este sentido, la manipulación de percepciones, la polarización política y la erosión de la legitimidad democrática se han convertido en objetivos estratégicos de primer orden para actores que buscan ventajas sin recurrir a la violencia tradicional.

¿Que hacer entonces?. La resiliencia social y la “alfabetización digital” se han convertido en la nueva "armadura" indispensable para el ciudadano moderno frente a los desafíos del ciberespacio. En un entorno donde la manipulación informativa y los ataques cognitivos buscan explotar debilidades colectivas, fortalecer la capacidad de discernimiento crítico y adaptabilidad social es fundamental para resistir intentos de desinformación y polarización.

La alfabetización digital no se limita a manejar herramientas tecnológicas, sino que implica comprender los riesgos, identificar noticias falsas, proteger los datos personales y participar activamente en la construcción de una cultura digital ética y responsable. Así, una sociedad resiliente y educada digitalmente tiene mayor capacidad para anticipar amenazas, responder de manera coordinada y preservar la cohesión social, blindando los valores democráticos ante la constante evolución del ciberconflicto.

El empleo de inteligencia artificial y la automatización han potenciado exponencialmente la efectividad de estas tácticas. Por un lado, la IA permite la creación de malware evolutivo y ataques automatizados capaces de adaptarse y evadir defensas en tiempo real. Por otro, dota a los equipos de ciberseguridad de herramientas capaces de analizar grandes volúmenes de datos, detectar anomalías y responder con rapidez y precisión. Este pulso tecnológico ha acelerado el ritmo del ciberconflicto y plantea un desafío constante a los Estados, empresas y ciudadanos: la necesidad de invertir en capacidades de vanguardia y en la actualización continua de sus estrategias y conocimientos.

Las implicaciones de esta transformación son profundas. La defensa nacional ya no puede limitarse a la protección de fronteras físicas o sistemas digitales; debe, además, blindar el tejido social frente a ataques que explotan la psicología colectiva y la información. Asimismo, la cooperación internacional, el intercambio de inteligencia y la formulación de marcos legales y éticos robustos se tornan imprescindibles para enfrentar amenazas que, por naturaleza, trascienden jurisdicciones y desafían los paradigmas clásicos de soberanía.

Finalmente, la ciberguerra, tal como se describe en el artículo, es un terreno en constante evolución donde la línea entre ataque y defensa es cada vez más difusa. Los Estados deben adoptar una postura proactiva, combinando “defensa avanzada” y “compromiso persistente” para anticipar y neutralizar amenazas antes de que se materialicen en daños reales, como lo subraya la estrategia del Departamento de Defensa de EE.UU. y los planteamientos de líderes como el General Nakasone. Sin embargo, la verdadera clave residirá en la capacidad de adaptarse, innovar y comprender que la competencia en el ciberespacio es permanente, multidimensional y, sobre todo, profundamente humana.

En suma, la ciberseguridad y la defensa nacional del siglo XXI exigen una visión integral, proteger infraestructuras, fortalecer capacidades técnicas, y, sobre todo, blindar a la sociedad frente a la manipulación y la desinformación. Solo así será posible preservar la estabilidad, la democracia y la confianza en un entorno global cada vez más interconectado y disputado.

Referencias

[1] Boletín del Centro Naval Nº 817(2007) Pág. 219 “La Guerra Informática” https://cefadigital.edu.ar/bitstream/1847939/1125/1/BCN-0817.pdf

[2] Paul M. Nakasone (2019) “A Cyber Force for Persistent Operations” . National Defense University Press . Pag 10 https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf

[3] MITRE ATT&CK MATRIX FOR ENTERPRISE (2022). https://attack.mitre.org/matrices/enterprise/

[4] Jeff Kosseff, (2019) The Contours of ‘Defend Forward’ Under International Law. CCDCOE (Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN). https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf

[5] NSO Group https://www.nsogroup.com/

[6] Black Cube https://www.blackcube.com/

[7] Dave Weinstein, (2018) “The Pentagon’s New Cyber Strategy: Defend Forward” LAWFARE. https://blog.google/threat-analysis-group/

[8] Irene Pujol (2024). “La guerra cognitiva convierte la mente en un campo de batalla”. Revista Española de Defensa, pag 48

[9] Gazula Mohan B. , (2017), Cyber Warfare Conflict Analysis and Case Studies, Cybersecurity Interdisciplinary Systems Laboratory (CISL)- Sloan School of Management, Room E62-422 - Massachusetts Institute of Technology.

[10] Brent Laura , (2019).NATO’s role in Cyberspace, February https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/ index.html

[11] Castillejos Arias Victor (2020) Aplicabilidad de los principios del derecho internacional humanitario a las acciones militares de los Estados en el ciberespacio. REVISTA ADLA Nº 05. p 205-213

[12] Cugnasco, C., Y. Becerra, J. Torres, E. Ayguadé, (2017) . Exploiting Key-Value Data Stores Scalability for HPC. 46th International Conference on Parallel Processing Workshops (ICPPW). Londres Junio 2017

[13] Colonial Pipeline Cyber Incident, U.S. Office of Cybersecurity, Energy Security, and Emergency Response, press release, Marzo 3, 2022 https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

[14] Chernenko E., Demidov, O., Lukyanov, F. (2018) Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms, Council on Foreign Relations (blog), Febrero 23. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

[15] Díaz del Río Durán Juan José , s.f. LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR. [Archivo PDF]. https://dialnet.unirioja.es /LaCiberseguridadEnElAmbitoMilitar-3837348.pdf
[16] De Vergara Evergisto, Trama Gustavo Adolfo (2017) OPERACIONES MILITARES CIBERNÉTICAS. Escuela Superior de Guerra Conjunta
[17] Dewar Robert S. , (2018) National Cybersecurity and Cyberdefense Policy Snapshots, CSS CYBER DEFENSE PROJECT.
[18] Diogenes Yuri, Ozkaya Erdal , (2020) Cybersecurity - Attack and Defense Strategies, 2da Edición, Revista PACKT.
[19] DOJ Press Conference Transcript October 19: Charges Against Russian Officers, Rev.com, Octubre 19, 2020